DEBATES ciberseguridad TIC

Detección y respuesta: cuando el reto ya no es ver el ataque, sino decidir qué hacer con él

SOPHOS

IR A PÁGINA SIGUIENTE

Detección y respuesta: cuando el reto ya no es ver el ataque, sino decidir qué hacer con él

La proliferación de entornos híbridos, la convergencia entre IT y OT, el crecimiento de la superficie de ataque, la presión regulatoria y la irrupción de la inteligencia artificial están obligando a las organizaciones a replantearse sus capacidades de detección y respuesta. Hoy el problema no suele ser la falta de alertas. De hecho, en muchas organizaciones ocurre justo lo contrario. El verdadero desafío consiste en interpretar correctamente la información disponible, entender el contexto de cada incidente y actuar con la suficiente rapidez para minimizar el impacto sobre el negocio.

Rosalía Arroyo

A esta complejidad se suma otro factor cada vez más evidente: la dificultad para mantener equipos especializados capaces de operar 24x7. En este contexto, Ciberseguridad TIC reunió en Bilbao a responsables de tecnología y ciberseguridad de diferentes organizaciones en un almuerzo ejecutivo patrocinado por Sophos con el fin de analizar el papel de los servicios de detección y respuesta gestionada (MDR). En este debate nos acompañaron José María Ortega, Global Technical Cybersecurity Architect de Abertis Mobility Services, la filial tecnológica

y centro de competencias digitales del Grupo Abertis; Albert Haro, Information Security Manager de la Agencia de ciberseguridad de Cataluña, organismo público encargado de proteger el ecosistema digital de toda la administración autonómica catalana; Marc García, Cybersecurity Manager del Ayuntamiento de Girona, que da servicio directo a una población de más de 100.000 habitantes y coordina una plantilla de más de mil empleados públicos; Sergi Ruiz, Responsable de Sistemas de Barcelona Activa, la agencia oficial de desarrollo económico del Ayuntamiento de Barcelona; Jordi Majadas, OT Manager de Laboratorios Reig Jofre, una compañía farmacéutica multinacional dedicada a la investigación, desarrollo, fabricación y comercialización de productos farmacéuticos y complementos alimenticios; junto con Álvaro Fernández, Sales Manager, y Guiu Ocón, Account Executive, de Sohos.

A lo largo del encuentro surgieron cuestiones tan relevantes como la falta de contexto en la gestión de alertas, la necesidad de responder fuera del horario laboral, el impacto de la IA en manos de los atacantes, la dificultad de coordinar múltiples proveedores o el papel que deben desempeñar los servicios gestionados en la protección de las organizaciones.

Detectar ya no es suficiente: el reto está en responder con criterio y a tiempo

La primera pregunta de la mesa parecía sencilla. ¿Cuál es hoy la principal preocupación en términos de detección y respuesta? Sin embargo, las respuestas dejaron claro que las organizaciones ya no perciben este desafío como una cuestión exclusivamente tecnológica. La visibilidad, la velocidad de reacción, la disponibilidad de recursos o la capacidad de análisis siguen siendo importantes, pero detrás de todos esos factores aparece un problema común: cómo mantener una capacidad real de respuesta en entornos cada vez más complejos.

José María Ortega, Txema, fue uno de los primeros en ponerlo sobre la mesa. Su organización ha optado por externalizar buena parte de las capacidades operativas de ciberseguridad, tanto las herramientas como los servicios asociados. En ese modelo, explicaba, la prioridad

> “En ciberseguridad ya no basta con detectar. Lo importante es entender qué está ocurriendo para reaccionar rápido y limitar el impacto antes de que el problema se extienda”
>
> **Txema Ortega,** Global Technical Cybersecurity Architect, **Abertis Mobility Services**

no es únicamente detectar una amenaza, sino contar con un proveedor capaz de acompañar a la organización durante todo el proceso de gestión del incidente. En su opinión, el valor

de un servicio gestionado reside precisamente en esa combinación de conocimiento técnico, inteligencia de amenazas y comprensión del negocio. “Tienen que estar al día de todo”, resumía, convencido de que el contexto y la capacidad de adaptación son tan importantes como la tecnología.

Albert Haro amplió esa visión desde la perspectiva de las administraciones públicas, donde la protección se articula alrededor de varios ejes simultáneos: los sistemas críticos, las personas, la gobernanza y la propia capacidad de respuesta. A su juicio, las organizaciones necesitan herramientas capaces de identificar comportamientos anómalos antes de que una amenaza llegue a materializarse, pero también mecanismos que permitan contener un incidente y recuperar la actividad con garantías cuando el ataque consigue superar las defensas. “Detectar antes de que pase y ser capaces de recuperarnos después” fue, en esencia, la idea que defendió durante su intervención. Porque, como recordaba, la detección únicamente tiene sentido si va acompañada de una capacidad real de respuesta.

> “No se puede proteger todo con la misma intensidad. Hay que priorizar los sistemas críticos, pero sin olvidar que muchas veces los atacantes terminan entrando por aquello que parecía menos importante”

Albert Haro, Information Security Manager, **Agencia de ciberseguridad de Cataluña**

Marc García llevó la conversación hacia una preocupación que apareció repetidamente durante el debate: la falta de recursos especializados, dejando claro el valor de servicios externos capaces de asumir tareas que internamente resultan difíciles de cubrir.

Los ataques no entienden de horarios y las organizaciones tampoco pueden mantener especialistas disponibles las veinticuatro horas del día. En ese contexto, explicaba, un servicio MDR permite delegar actividades como la recolección de logs, el análisis de alertas o la investigación inicial de incidentes, apoyándose en procedimientos sencillos y previamente acordados.

La intervención de Jordi Majadas introdujo además otro elemento que acabaría apareciendo varias veces durante la jornada: la complejidad creciente de los entornos híbridos: la convivencia entre IT, OT, cloud y múltiples proveedores multiplica las dificultades operativas y exige capacidades muy especializadas.

A su juicio, el problema no es únicamente disponer de herramientas. También es necesario contar con procedimientos maduros, playbooks claros y profesionales capaces de interpretar correctamente lo que está ocurriendo. “Hoy en día herramientas hay muchas”, reconocía, pero disponer

> “Lo que valoramos de un servicio MDR es que funcione: que sea sencillo de desplegar, que minimice los falsos positivos y que cuando te llamen sea porque han detectado algo que realmente merece atención”

Marc García,
Cybersecurity Manager, **Ayuntamiento de Girona**

de personas preparadas para investigar y responder sigue siendo uno de los mayores desafíos.

La conversación dejó también calro que los sistemas OT siguen planteando retos muy distintos a los del mundo IT tradicional. La prioridad en OT continúa siendo la disponibilidad de la producción, lo que limita enormemente las posibilidades de actuación ante determinados incidentes. “No puedes hacer una actuación tan agresiva en OT como puedes hacer en IT”, advertía el OT Manager de Laboratorios Reig Jofre. En algunos casos, aislar un sistema o detener un proceso puede tener consecuencias económicas inmediatas. Además, se trata de entornos con ciclos de vida muy largos, equipos difíciles de actualizar y una creciente conectividad que aumenta la superficie de exposición.

Precisamente por ello, varios participantes insistieron en la importancia de que cualquier proveedor externo conozca perfectamente qué puede hacer, qué no puede hacer y cuáles son los límites operativos de cada entorno. En determinadas instalaciones, una decisión incorrecta puede traducirse en la paralización de una línea de producción o en pérdidas económicas significativas en cuestión de minutos.

El verdadero cuello de botella ya no es la tecnología

Si en la primera parte del debate la conversación giró alrededor de la complejidad operativa de la detección y respuesta, la segunda permitió profundizar en una cuestión aún más relevante: dónde están realmente los límites de las organizaciones cuando tienen que enfrentarse a una amenaza.

La respuesta fue bastante unánime. Más allá de herramientas concretas o de nuevas capacidades tecnológicas, el principal problema sigue siendo la disponibilidad de talento especializado. Albert Haro fue especialmente claro al respecto. A su juicio, la escasez de profesionales de ciberseguridad se ha convertido en uno de los grandes desafíos para organizaciones públicas y privadas. “Falta mucho profesional”, aseguraba, recordando que la demanda de especialistas ha crecido a un ritmo muy superior a la capacidad de formación del sector y que el reto de fondo sigue siendo encontrar personas con los conocimientos necesarios para operar entornos cada vez más complejos.

Marc García reconocía que, para su organización, la prioridad sigue siendo detectar los ataques lo antes posible. Cuanto antes se identifica una amenaza, mayores son las posibilidades de contenerla antes de que genere un impacto relevante. Sin embargo, también advertía de que detectar ya no es suficiente y que las organizaciones reciben hoy una cantidad de información difícil de gestionar internamente. Por eso considera que uno de los principales valores de un servicio MDR reside precisamente en aportar contexto. Mientras un SIEM tradicional permite recopilar y correlacionar información, el MDR añade una capa adicional de análisis e interpretación que ayuda a entender qué está ocurriendo realmente y cuál debería ser la respuesta más adecuada.

La misma idea apareció en la intervención de Sergi Ruiz, aunque desde una perspectiva diferente. Para él, la detección inicial es cada vez menos problemática gracias a las capacidades de las herramientas actuales. El verdadero cuello de botella aparece después: "¿Qué hago ahora? ¿Cómo detengo esto? ¿Cómo lo corrijo?", planteaba, describiendo una situación habitual en muchas organizaciones. Aunque una alerta llegue a tiempo, responder correctamente exige experiencia, conocimiento especializado y capacidad de actuación bajo presión.

> "La tecnología por sí sola no resuelve el problema. Lo que marca la diferencia son los procesos, la capacidad de respuesta y disponer de personas con experiencia capaces de tomar decisiones"
>
> **Jordi Majadas,**
> OT Manager, **Laboratorios Reig Jofre**

A diferencia de un equipo interno, que puede enfrentarse a situaciones de este tipo de forma esporádica, un equipo especializado de respuesta trabaja continuamente con incidentes reales. Esa experiencia acumulada, defendía, permite actuar con mayor rapidez, mantener la cabeza fría y aportar conocimientos que difícilmente pueden mantenerse dentro de una organización cuya actividad principal no es la ciberseguridad.

La reflexión conectó rápidamente con la intervención de Jordi Majadas, quier defendió que disponer de herramientas no garantiza necesariamente una respuesta eficaz. "La tecnología detecta", afirmaba, añadiendo que lo verdaderamente diferencial es contar con procesos claros y con personas capaces de interpretarlos y ejecutarlos cuando se produce un incidente. Por eso situaba los procesos y los recursos especializados por delante de la propia tecnología como factores críticos para mejorar la capacidad de respuesta.

Una visión muy similar compartía Txema Ortega. Para él, detectar y comprender un ataque

"Detectar un incidente es sólo el principio. El verdadero reto aparece cuando hay que decidir cómo contenerlo, cómo recuperarse y cómo hacerlo con criterio en medio de una situación de máxima presión"

Sergi Ruiz,
Responsable de Sistemas, **Barcelona Activa**

La falta de profesionales especializados se ha convertido en uno de los principales factores que está impulsando la adopción de servicios MDR

son dos caras de la misma moneda. Tan problemático es no ver una amenaza como no entender qué está ocurriendo una vez que se ha detectado. Además, advertía que los ataques evolucionan constantemente y obligan a trabajar cada vez más sobre patrones de comportamiento y capacidades avanzadas de análisis. "Lo que hoy es válido mañana cambia", recordaba, defendiendo la necesidad de apoyarse en tecnologías capaces de adaptarse a esa evolución continua.

Sin embargo, cuando la conversación volvió a la adopción de servicios MDR, el Global Cybersecurity Technical Architect de Abertis Mobility Services no tuvo dudas sobre cuál era el factor decisivo: los recursos.

A su juicio, construir internamente todas las capacidades necesarias para operar un servicio avanzado de detección y respuesta exige incorporar múltiples perfiles especializados —analistas, expertos en vulnerabilidades, responsables de inteligencia o gestores de operación— cuyo coste resulta difícil de asumir para muchas organizaciones.

Pero el problema no termina ahí. Incluso disponiendo del presupuesto necesario, el conocimiento se vuelve rápidamente obsoleto en un sector que evoluciona a gran velocidad. Mantener actualizados todos esos perfiles supone una inversión continua que muchas compañías prefieren trasladar a proveedores especializados.

Las intervenciones encontraron eco inmediato en los representantes de Sophos. Guiu Ocón destacaba precisamente el valor que aportan los servicios especializados cuando las organizaciones necesitan acceder a conocimientos muy específicos, experiencia en gestión de incidentes y capacidad de respuesta en situaciones

de alta presión. A su juicio, la ciberseguridad ha evolucionado desde un modelo centrado en productos hacia otro claramente orientado a servicios, donde el verdadero valor ya no está únicamente en la herramienta, sino en las personas que la operan.

Álvaro Fernández reforzó esa idea recordando que muchas organizaciones ya no contemplan el MDR únicamente como una tecnología adicional, sino como una extensión de sus propios equipos de seguridad. En algunos casos, explicaba, el servicio llega a convertirse prácticamente en el departamento de ciberseguridad de la organización. En otros, actúa como complemento a SOC internos o externos ya existentes. En ambos escenarios, el denominador común sigue siendo el mismo: acceder a capacidades especializadas de forma más rápida, eficiente y económicamente viable que construyéndolas desde cero.

Porque si algo quedó claro durante esta parte del debate es que el reto está en disponer de las personas, los procesos y el conocimiento necesarios para interpretarlas y responder cuando realmente importa.

Cuánto contexto necesita realmente un proveedor para proteger una organización

La conversación avanzó entonces hacia una cuestión especialmente sensible para cualquier responsable de seguridad: cuánto contexto necesita realmente un proveedor externo para poder responder con criterio cuando se produce un incidente; ¿hasta qué punto están dispuestas las organizaciones a compartir información sobre sus infraestructuras, procesos y activos críticos con un tercero?

Las respuestas mostraron matices interesantes. Marc García, cuya organización ya trabaja con un servicio MDR, defendió que precisamente una de las ventajas de este modelo es reducir parte de la carga de mantenimiento que tradicionalmente han exigido los SOC. Según explicaba, para que un SOC funcione correctamente es necesario suministrar y mantener actualizada una gran cantidad de información sobre la organización. En su experiencia, el MDR les ha permitido obtener valor con una necesidad mucho menor de parametrización continua. Además, destacaba otro aspecto que considera diferencial: el acceso a la experiencia acumulada por un proveedor que observa amenazas en

> “Cada vez más clientes nos piden integrar dentro de la estrategia de detección y respuesta entornos OT, IoT y sistemas que históricamente habían quedado fuera de los modelos tradicionales de seguridad”

Guiu Ocón,
Account Executive, **Sophos**

múltiples organizaciones y sectores. Esa visión global, afirmaba, permite reaccionar antes ante amenazas emergentes y mejorar la respuesta frente a ataques complejos o vulnerabilidades de día cero.

La capacidad de actuación fue precisamente otro de los elementos que más interés despertó durante el debate. Sergi Ruiz coincidía en que el valor de un MDR aparece cuando es capaz de ir más allá de la monitorización y participar activamente en la contención de un incidente. Mientras que un SOC puede aportar visibilidad y análisis, un MDR incorpora la posibilidad de aislar equipos comprometidos, bloquear dispositivos o distribuir indicadores de compromiso con rapidez. “Esa capacidad de respuesta no siempre se proporciona”, advertía.

Sin embargo, no todos los asistentes planteaban la cuestión en términos de sustitución. Jordi rechazó presentar SOC y MDR como modelos enfrentados y defendió una aproximación más complementaria. “Los dos productos pueden llevarse bien entre ellos”, resumía. Desde su punto de vista, la cuestión no consiste tanto en elegir entre uno u otro como en definir correctamente el papel que debe desempeñar cada servicio dentro de la operación de seguridad.

> “Las organizaciones necesitan alinear tecnología, procesos y personas. Las herramientas pueden detectar amenazas, pero sin equipos especializados que interpreten esas señales resulta muy difícil responder con eficacia”
>
> **Álvaro Fernández,**
> Sales Manager, **Sophos**

Esa misma lógica aplicaba al contexto. Jordi Majadas defendía compartir la información necesaria para que el proveedor pueda operar correctamente, pero siempre bajo criterios de mínimo privilegio. Es decir, facilitar acceso a aquello que realmente aporta valor sin abrir de forma indiscriminada toda la infraestructura.

Txema Ortega, por el contrario, se mostró más partidario de una colaboración profunda con aquellos proveedores que desempeñan un papel crítico en la protección de la organización. Su razonamiento era sencillo: si se espera que un proveedor ayude a tomar decisiones relevantes durante un incidente, necesita conocer adecuadamente el entorno. “Cuanta menos información le dé, peor para mí”, afirmaba. De hecho, relativizaba la complejidad del proceso y explicaba que, en su experiencia, compartir la información necesaria había resultado mucho más sencillo de lo que inicialmente esperaba.

La visión de Albert Haro aportó una perspectiva diferente, marcada por la realidad de las grandes administraciones públicas. En entornos donde conviven miles de sistemas y múltiples organismos conectados, resulta evidente que ningún

proveedor puede actuar eficazmente sin disponer de un nivel mínimo de conocimiento del entorno. “Si no tienes información, luego no podrás actuar”, resumía. No obstante, coincidía en que la clave está en identificar qué información resulta realmente necesaria para operar y cuál puede permanecer dentro de la organización.

Más allá de los distintos matices, el debate terminó dejando una conclusión bastante clara. Lejos de presentarse como alternativas incompatibles, SOC y MDR aparecieron repetidamente como modelos complementarios. Incluso desde Sophos se insistió en esa idea. Como explicaba Guiu Ocón, ambos enfoques responden a necesidades distintas y pueden convivir dentro de una misma estrategia. El MDR aporta especialización y capacidad de respuesta, mientras que el SOC mantiene una visión más amplia de la operación.

De la alerta a la acción: qué esperan realmente las organizaciones de un MDR

Después de hablar de talento, contexto, procesos y modelos operativos, la conversación terminó aterrizando en una cuestión mucho más práctica: qué esperan realmente las organizaciones cuando contratan un servicio MDR.

> La ciberseguridad está evolucionando desde modelos basados en herramientas hacia modelos basados en servicios

Y las respuestas fueron llamativamente coincidentes. Ningún participante empezó hablando de inteligencia artificial, correlación de eventos o automatización avanzada. Lo que apareció una y otra vez fueron conceptos como acompañamiento, cercanía, capacidad de actuación y continuidad operativa.

Para Sergi Ruiz, el valor empieza por la relación entre cliente y proveedor. Más allá de la tecnología, espera que exista una interacción fluida y una capacidad real de acompañamiento cuando se produce un incidente relevante. “Que la interacción sea fácil”, resumía. Porque cuando la situación se complica, lo que realmente marca la diferencia es contar con alguien que ayude a interpretar lo que está ocurriendo y acompañe al equipo durante todo el proceso. Apostaba claramente el directivo por un servicio “que te acompañe en el proceso y no se quede simplemente en la transmisión de una alerta”.

Jordi Majadas compartía esa visión, aunque añadía un elemento que considera igual de importante: la capacidad de entender el negocio. En su opinión, un MDR debe conocer no solo la infraestructura tecnológica, sino también el impacto que determinadas decisiones pueden tener sobre la operación. “No solo la infraestructura, también el negocio”, insistía, recordando que una respuesta técnicamente correcta no siempre es la más adecuada desde el punto de vista operativo.

Sin embargo, la experiencia práctica de Txema Ortega introdujo un matiz interesante. Desde su punto de vista, existen escenarios en los que el conocimiento detallado del negocio no es necesariamente imprescindible para actuar con eficacia. En amenazas claramente identifica-

das, explicaba, disponer de suficiente contexto técnico puede ser más que suficiente para tomar decisiones rápidas. Como ejemplo relató cómo, durante un ejercicio de pentesting, el MDR detectó automáticamente una máquina Kali y la aisló antes incluso de contactar con él. “Bloquearon la máquina y luego me pusieron el caso”, recordaba.

Precisamente esa capacidad de actuación fue uno de los temas que más interés generó durante la conversación. Álvaro Fernández explicó que los niveles de intervención pueden adaptarse a las necesidades de cada organización: hay clientes que prefieren mantener el control sobre determinadas decisiones y otros que buscan una respuesta mucho más autónoma por parte del proveedor. “Tú puedes definir también la forma de actuar”, señalaba, describiendo distintos modelos de operación basados en procedimientos previamente acordados.

La integración apareció también como otro requisito recurrente. Albert Haro explicaba que, en organizaciones grandes y complejas, el MDR no suele sustituir a los mecanismos ya existentes. Lo que se espera es que complemente las capacidades disponibles y encaje dentro de una visión más amplia de la seguridad. “Necesitamos que diferentes soluciones se integren con nuestra manera de hacer”, resumía.

Marc García llevó el debate nuevamente al terreno más práctico. Lo que él espera de un MDR es, sencillamente, que funcione. Detrás de esa afirmación aparentemente simple hay varios requisitos muy concretos: facilidad de despliegue, bajo impacto sobre los equipos internos, reducción de falsos positivos y capacidad para detectar incidentes reales cuando realmente importa. “He contestado llamadas del MDR a la

una de la mañana y a las cuatro de la mañana, y han sido casos reales", explicaba.

Esa reflexión permitió a Guiu Ocón introducir uno de los grandes retos de cualquier servicio de detección y respuesta: separar el ruido de las señales relevantes. A su juicio, buena parte del valor actual del MDR reside precisamente en esa capacidad para filtrar millones de eventos, identificar aquello que realmente requiere atención y reducir la fatiga que generan los falsos positivos. Un trabajo que combina automatización, inteligencia artificial y experiencia acumulada por los equipos de analistas.

Además, señalaba que la conversación ya está empezando a desplazarse hacia nuevos escenarios. Cada vez más organizaciones preguntan cómo extender estas capacidades a dispositivos IoT, sistemas industriales y otros entornos tradicionalmente alejados de las plataformas de seguridad convencionales. Una evolución que, según explicó, se ha acelerado especialmente tras la integración de Secureworks dentro de Sophos.

El cierre del debate permitió condensar buena parte de las conclusiones de la jornada. Álvaro Fernández defendió que todas las organizaciones necesitan capacidades de detección y respuesta, independientemente de cómo decidan obtenerlas. En ese contexto, destacó tres elementos diferenciales de la propuesta de Sophos: la inteligencia obtenida de una enorme base instalada global, la capacidad de operar sobre tecnologías de terceros sin obligar a sustituir inversiones existentes y una adopción sencilla que reduzca las barreras de entrada.

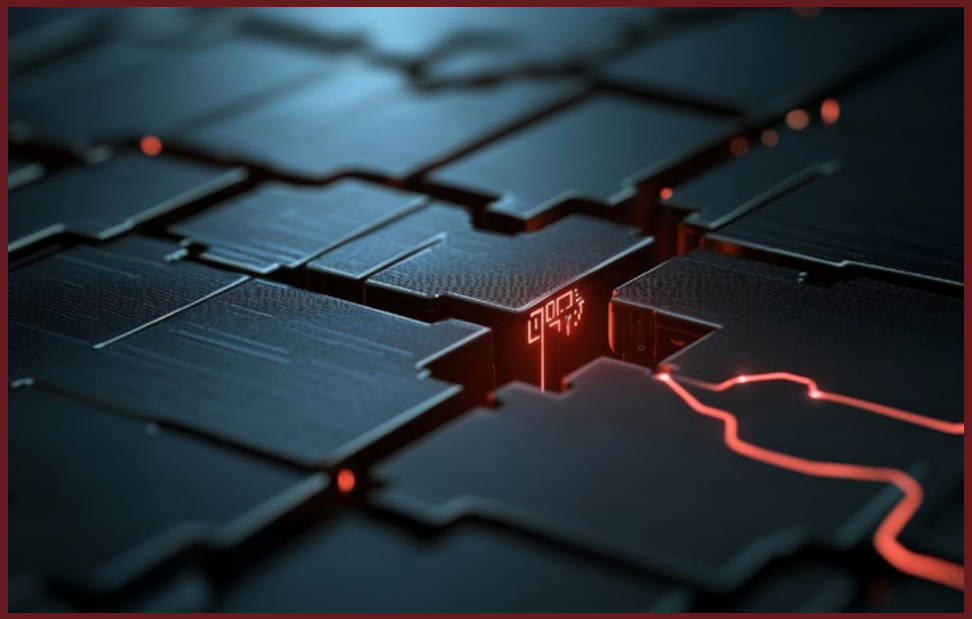
Pero más allá de las características concretas de una plataforma o de un servicio, la conversación dejó claro que las organizaciones ya no buscan únicamente herramientas capaces de detectar amenazas. Lo que necesitan es disponer de los recursos, la experiencia y la capacidad de actuación necesarios para responder cuando el incidente llega.

Sophos MDR: contexto, experiencia y capacidad de respuesta para complementar la operación de seguridad

La propuesta MDR de Sophos parte de una idea que apareció de forma recurrente durante el debate: detectar una amenaza es solo una parte del problema. Tan importante como identificar una alerta es disponer del contexto, la experiencia y la capacidad de actuación necesarios para responder con rapidez y criterio cuando se produce un incidente.

Según explicaron Guiu Ocón y Álvaro Fernández, el objetivo del servicio es ayudar a las organizaciones a complementar sus capacidades de seguridad mediante una combinación de tecnología, inteligencia de amenazas y equipos especializados que operan de forma continua. La propuesta está diseñada para adaptarse a distintos niveles de madurez y busca dar respuesta a algunos de los retos que más preocuparon a los asistentes, como la escasez de recursos especializados, la necesidad de operar fuera del horario laboral o la dificultad de interpretar correctamente señales procedentes de entornos cada vez más complejos.

Uno de los aspectos más destacados durante la conversación fue la importancia del contexto. A juicio de Sophos, la eficacia de cualquier servicio de detección y respuesta depende en gran medida de su capacidad para entender cómo funciona cada organización, cuáles son sus activos críticos y qué impacto tendría una determinada acción sobre el negocio. Por ese motivo, el servicio se apoya en un proceso de adaptación al entorno



del cliente que permite definir procedimientos, niveles de actuación y mecanismos de escalado acordes con cada realidad operativa.

Desde el punto de vista tecnológico, Sophos MDR es capaz de recopilar y correlacionar información procedente de múltiples fuentes, tanto de soluciones propias como de terceros. Esta aproximación permite ofrecer una visión más amplia del entorno de seguridad y facilita la investigación de incidentes que afectan simultáneamente a distintos vectores, desde endpoints y servidores hasta identidades, redes o entornos cloud.

> Los ataques son cada vez más rápidos, más automatizados y más difíciles de interpretar; el problema no es únicamente detectarlos, sino entender qué está ocurriendo antes de que el impacto alcance al negocio

Otro de los elementos diferenciales señalados por la compañía es la experiencia acumulada por sus equipos de analistas. El servicio se nutre de la observación continua de amenazas en miles de organizaciones

de distintos sectores y geografías, lo que permite identificar patrones de ataque emergentes y trasladar ese conocimiento a los clientes. Esta inteligencia global resulta especialmente valiosa ante amenazas cada vez más rápidas, automatizadas y apoyadas en inteligencia artificial.

La evolución de la oferta también incorpora capacidades adicionales orientadas a abordar algunos de los vectores que más preocupan actualmente a las organizaciones, como la exposición a vulnerabilidades o el compromiso de identidades. Todo ello con un objetivo común: reducir la carga operativa de los equipos internos, mejorar la velocidad de respuesta y ayudar a las organizaciones a mantener el control incluso en escenarios complejos donde la disponibilidad de recursos especializados es limitada.

En un momento en el que la discusión ya no gira únicamente alrededor de detectar amenazas, sino de responder con rapidez y criterio, Sophos plantea el MDR como una herramienta para complementar las capacidades existentes y aportar experiencia operativa allí donde más difícil resulta mantenerla de forma interna.